A

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/965,907	09/27/2001	Guy Tsafnat	NA01-17001	4240

28875 7590 09/19/2005

Zilka-Kotab, PC
P.O. BOX 721120
SAN JOSE, CA 95172-1120

EXAMINER	
REVAK, CHRISTOPHER A	
ART UNIT	**PAPER NUMBER**
2131	

DATE MAILED: 09/19/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 09/965,907	**Applicant(s)** TSAFNAT ET AL.
	Examiner Christopher A. Revak	**Art Unit** 2131

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *9/27/01*.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-27* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-27* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) □ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application (PTO-152)

6) □ Other: _____.

DETAILED ACTION

Claim Rejections - 35 USC § 102

1. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

2. Claims 1-5,7-14,16-23, and 25-27 are rejected under 35 U.S.C. 102(e) as being anticipated by Munson et al, U.S. Patent 6,681,331.

As per claim 1, the teachings of Munson et al discloses of a method for detecting a denial-of-service attack using an execution profile for a kernel of a server computer system, comprises producing a run-time execution profile by gathering statistics related to execution of a protocol stack within the kernel of the server, wherein the protocol stack processes packets received from client computer systems, comparing the run-time execution profile with a normal execution profile for the kernel of the server, wherein the normal execution profile is representative of execution when the server is not subject to a denial-of-service attack, and indicating that a denial-of-service attack is taking place if the run-time execution profile deviates from the normal execution profile (col. 1, lines 54-57; col. 3, lines 34-59; and col. 4, lines 26-37).

As per claims 2,11, and 20, Munson et al teaches of producing the run-time execution profile involves gathering statistics regarding a fraction of time that the server spends executing one or more portions code related to the protocol stack (col. 3, lines 34-59 and col. 6, lines 14-25).

As per claims 3,12, and 21, Munson et al discloses of producing the run-time execution profile involves producing a vector indicating a number of times that the server is found to be executing the one or more portions of code related to the protocol stack (col. 4, lines 26-65).

As per claims 4,13, and 22, Munson et al discloses of portions of code related to the protocol stack include a portion related to processing TCP SYN requests, a portion related to processing TCP ACKs, a portion related to processing TCP data, a portion related to processing ICMP echo requests, and a portion that is unrelated to the protocol stack (col. 3, lines 34-59).

As per claims 5,14, and 23, it is recited by Munson et al of producing the normal execution profile by gathering statistics related to execution of the server when the server is not subject to a denial-of-service attack (col. 4, lines 37-43).

As per claims 7,16, and 25, it is taught by Munson et al of producing the run-time execution profile involves gathering statistics over a first time window, and subsequently gathering statistics for a subsequent run-time execution profile over a second time window (col. 3, lines 34-59 and col. 6, lines 14-25).

As per claims 8,17, and 26, Munson et al teaches of gathering statistics for a concurrent execution profile over a concurrent time window that overlaps the first time window and the second time window, so that a denial-of service attack that overlaps the first time window and the second time window can be detected in the concurrent time window (col. 3, lines 34-59 and col. 6, lines 14-25).

As per claims 9,18, and 27, Munson et al discloses of comparing the run-time execution profile with the normal execution profile involves determining if the run-time execution profile deviates more than a pre-specified amount from the normal execution profile (col. 4, lines 40-65).

As per claim 10, Munson et al recites of a computer-readable storage medium storing instructions that when executed by a computer cause the computer to perform a method for detecting a denial-of-service attack using an execution profile for a kernel of a server computer system, the method comprising producing a run-time execution profile by gathering statistics related to execution of a protocol stack within the kernel of the server, wherein the protocol stack processes packets received from client computer systems, comparing the run-time execution profile with a normal execution profile for the kernel of the server, wherein the normal execution profile is representative of execution when the server is not subject to a denial-of-service attack, and indicating that a denial-of-service attack is taking place if the run-time execution profile deviates from the normal execution profile (col. 1, lines 54-57; col. 3, lines 34-59; and col. 4, lines 26-37).

As per claim 19, Munson et al teaches of an apparatus that detects a denial-of-service attack through use of an execution profile for a kernel of a server computer system, comprising a profiling mechanism that is configured to produce a run-time execution profile by gathering statistics related to execution of a protocol stack within the kernel of the server, wherein the protocol stack processes packets received from client computer systems, a comparison mechanism that is configured to compare the run-time execution profile with a normal execution profile for the kernel of the server, wherein the normal execution profile is representative of execution when the server is not subject to a denial-of-service attack, and wherein the comparison mechanism is configured to indicate that a denial-of-service attack is taking place if the run-time execution profile deviates from the normal execution profile (col. 1, lines 54-57; col. 3, lines 34-59; and col. 4, lines 26-37).

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claims 6,15, and 24 are rejected under 35 U.S.C. 103(a) as being unpatentable over Munson et al, U.S. Patent 6,681,331.

As per claims 6,15, and 24, it is disclosed by Munson et al that if a denial-of-service attack is detected, the method further comprises sending an alarm (col. 5, lines 18-30). The teachings of Munson et al are silent in disclosing of blocking offending packets from reaching the server. The examiner hereby takes official notice the use of dropping suspicious packets is notoriously well known. It would have been obvious to a person of ordinary skill in the art at the time of the invention to have been motivated to stop suspicious communication from being further processed by blocking them from being sent. The motivational benefits of blocking offending packets is so that they are not allowed to be passed since they are known to be suspicious and can perform actions that are undesirable. It is obvious that the teachings of Munson et al would have allowed packets to be blocked if they were deemed to be suspicious so that they can no longer perform malicious operations.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Christopher A. Revak whose telephone number is 571-272-3794. The examiner can normally be reached on Monday-Friday, 6:30am-3:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Christopher Revak
Primary Examiner
AU 2131
9/16/05

CR
September 16, 2005